wherein the network telephony connection server determines the telephone identifier for the callee identified in the callee user identifier and sends the response message to the callee at the telephone identifier.

- Appendix A contains a marked-up version of the claim above indicating the amendments to the claim.

In the application-as-filed, Applicant inadvertently included two Claim "10's". Please cancel the second instance of originally filed Claim 10 as follows without prejudice to further prosecution of the subject matter of the claims. Claim 13 is added below to correct the duplicate claim numbering.

10. (Cancel) The system of Claim 7 wherein the response and request messages are communicated by the network telephony connection server in accordance with the MGCP protocol.

Please add new Claims 13-30 as follows:

13. (New) The system of Claim 7 wherein the response and request messages are communicated by the network telephony connection server in accordance with the MGCP protocol.

14. (New) A method of enabling encryption/authentication on a data network telephony system including a plurality of Portable Information Devices (PIDs) coupled to data network telephones within the data network telephony system, the method comprising in combination:

transmitting a request from a first PID to a second PID for encryption/authentication data associated with the second PID;

responding to the request by transmitting the encryption/authentication data associated with the second PID from the second PID to the first PID;

receiving the encryption/authentication data associated with the second PID at the first PID;

storing the encryption/authentication data associated with the second PID in an address book entry in the first PID;

transmitting encryption/authentication data associated with the first PID from the first PID to the second PID;

receiving the encryption/authentication data associated with the first PID at the second PID;

storing the encryption/authentication data associated with the first PID in an address book entry in the second PID; and

transmitting an acknowledgement message from the second PID to the first PID acknowledging receipt of the encryption/authentication data associated with the first PID.

15. (New) The method of Claim 14 wherein responding to the request includes the second PID transmitting public key information for an asymmetric cryptography system to the first PID.

16. (New) The method of Claim 14 wherein the transmitted encryption/authentication data associated with the first PID includes a confirmation message to acknowledge receipt of the encryption/authentication data associated with the second PID.

McDonnell Boehnen Hulbert & Berghoff
300 South Wacker Drive, 32nd Floor
Chicago, IL 60606
(312)913-0001

17. (New) The method of Claim 16 wherein the confirmation message includes a copy of the encryption/authentication data associated with the second PID to verify that the encryption/authentication data associated with the second PID was received.

18. (New) The method of Claim 14 wherein the request includes the encryption/authentication data associated with the first PID.

19. (New) A method for resolving a shared secret on a data network telephony system, the data network telephony system comprising a plurality of Portable Information Devices (PIDs) coupled to data network telephones within the data network telephony system, the method comprising in combination:

transmitting a suggested shared secret to one or more PIDs from a first PID;

receiving the suggested shared secret on the one or more PIDs; and

confirming the suggested shared secret by sending at least one acknowledgement message from the one or more PIDs to the first PID.

20. (New) The method of Claim 19 wherein the suggested shared secret is generated by a random-number generator within the first PID.

21. (New) The method of Claim 19 wherein the suggested shared secret is generated by a pseudo-random-number generator the first PID.

McDonnell Boehnen Hulbert & Berghoff
300 South Wacker Drive, 32nd Floor
Chicago, IL 60606
(312)913-0001

22. (New) The method of Claim 19 wherein the suggested shared secret is selected from the group consisting of encryption/authentication data, and encryption/decryption data.

23. (New) The method of Claim 19 further comprising rejecting the suggested shared secret by at least one of the one or more PIDs and suggesting an alternative shared secret by the first PID prior to accepting the suggested shared secret at each of the one or more PIDs.

24. (New) The method of Claim 19 wherein the suggested shared secret is accepted by at least one of the one or more PIDs by meeting a predetermined length requirement.

25. (New) The method of Claim 19 further comprising transmitting a plurality of suggested shared secrets to at least one of the one or more PIDs by the first PID prior to confirming the suggested shared secret at the one or more PIDs.

26. (New) The method of Claim 25 wherein at least one of the one or more PIDs selects one of the plurality of suggested shared secrets based on criteria selected from the group consisting of a suggested shared secret length, a suggested shared secret alphanumeric character redundancy, a suggested shared secret averaging, a timestamp of transmission of suggested shared secrets, and a pre-selection of suggested shared secrets.

27. (New) The method of Claim 26 further comprising agreeing upon a selected suggested shared secret by at least one of the one or more PIDs and storing the agreed upon selected suggested shared secret.

McDonnell Boehnen Hulbert & Berghoff
300 South Wacker Drive, 32nd Floor
Chicago, IL 60606
(312)913-0001